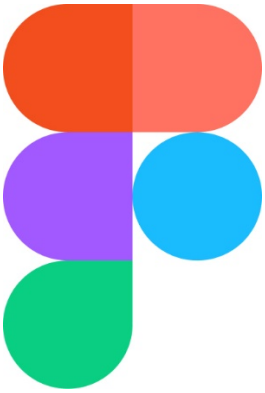

Figma, Inc.

System and Organization Controls (SOC) 3 Report

Report on Figma System

Based on the Trust Services Criteria for Security

For the Period November 1, 2019 through October 31, 2020

Figma
116 New Montgomery Street, Ste 400
San Francisco, CA 94105

Management's Report of its Assertions on the Effectiveness of Its Controls Over the Figma System Based on the Trust Services Criteria for Security

We, as management of, Figma, Inc. are responsible for:

- Identifying the Figma System ("System") and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Subservice Organizations Matters

Figma uses Amazon Web Services ("AWS") to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The System (Attachment A) includes only the controls of Figma and excludes controls of the sub-service organization. The Description also indicates that certain trust services criteria specified therein can be met only if the sub-service organization controls assumed in the design of Figma's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of sub-service organization.

However, we perform annual due diligence procedures for third-party sub-service provider and based on the procedures performed, nothing has been identified that prevents us from achieving its specified service commitments.

Very truly yours,

Praveer Melwani
Director, Business Operations & Finance

Ernst & Young LLP
18101 Von Karman Ave
Irvine, CA 92612

Tel: +1 949 794 2300
ey.com

Building a better working world

Report of Independent Accountants

To the Management of Figma, Inc.

Scope

We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls Over the Figma System Based on the Trust Services Criteria for Security ("Assertion"), that Figma's controls over the Figma System ("System") were effective throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Figma uses Amazon Web Services ("AWS") to provide physical safeguards, environmental safeguards, infrastructure support and management, and storage services. The System (Attachment A) indicates that Figma's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if AWS' controls, assumed in the design of Figma's controls, are suitably designed and operating effectively along with related controls at the service organization. The System presents the Figma System and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our examination did not extend to the services provided by AWS, and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period November 1, 2019 to October 31, 2020.

Management's Responsibilities

Figma's management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Figma System ("System") and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Figma's relevant security policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Figma's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Figma's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Figma's controls over the system were effective throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Building a better working world

Restricted use

This report is intended solely for the information and use of Figma and user entities of Figma System and is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

Irvine, California

December 9, 2020

Figma
116 New Montgomery Street, Ste 400
San Francisco, CA 94105

Attachment A

Figma Service Organization's
Description of the Boundaries of Figma

Company Overview and Background

Figma (the "Company") is a privately held company headquartered in San Francisco, California, which was founded in 2012. The Figma application ("Figma") is a web-based interface design tool that allows users to easily create and securely share interface and application designs. Figma has been adopted by many organizations ranging from startups to large multinational organizations.

Overview of Products and Service

A defining characteristic of Figma is that it allows multiple users to collaborate in real time as they work on user interface designs.

Infrastructure

Figma operates as a Software-as-a-Service ("SaaS") solution hosted in a public cloud. The infrastructure is hosted and managed on Amazon Web Services ("AWS") in the United States across multiple regions and availability zones to support fault tolerance, high availability, and disaster recovery. AWS operates under a shared responsibility model. Under this model, Figma uses AWS for services related to server hosting, physical and environmental protection, network management, and disk storage supporting the System.

The System is based on a multi-tenant architecture that applies common and consistent management processes and controls to all customers. The infrastructure has been designed to provide high availability and all critical infrastructure components are redundant across multiple AWS availability zones. Web servers and databases are deployed in multiple availability zones each consisting of one or more discrete data centers, with fully redundant power, networking, and connectivity housed in separate secured facilities. The System is built on Linux servers and runs on an Amazon's Relational Database Service ("RDS") database. The following diagram shows major components of the System.

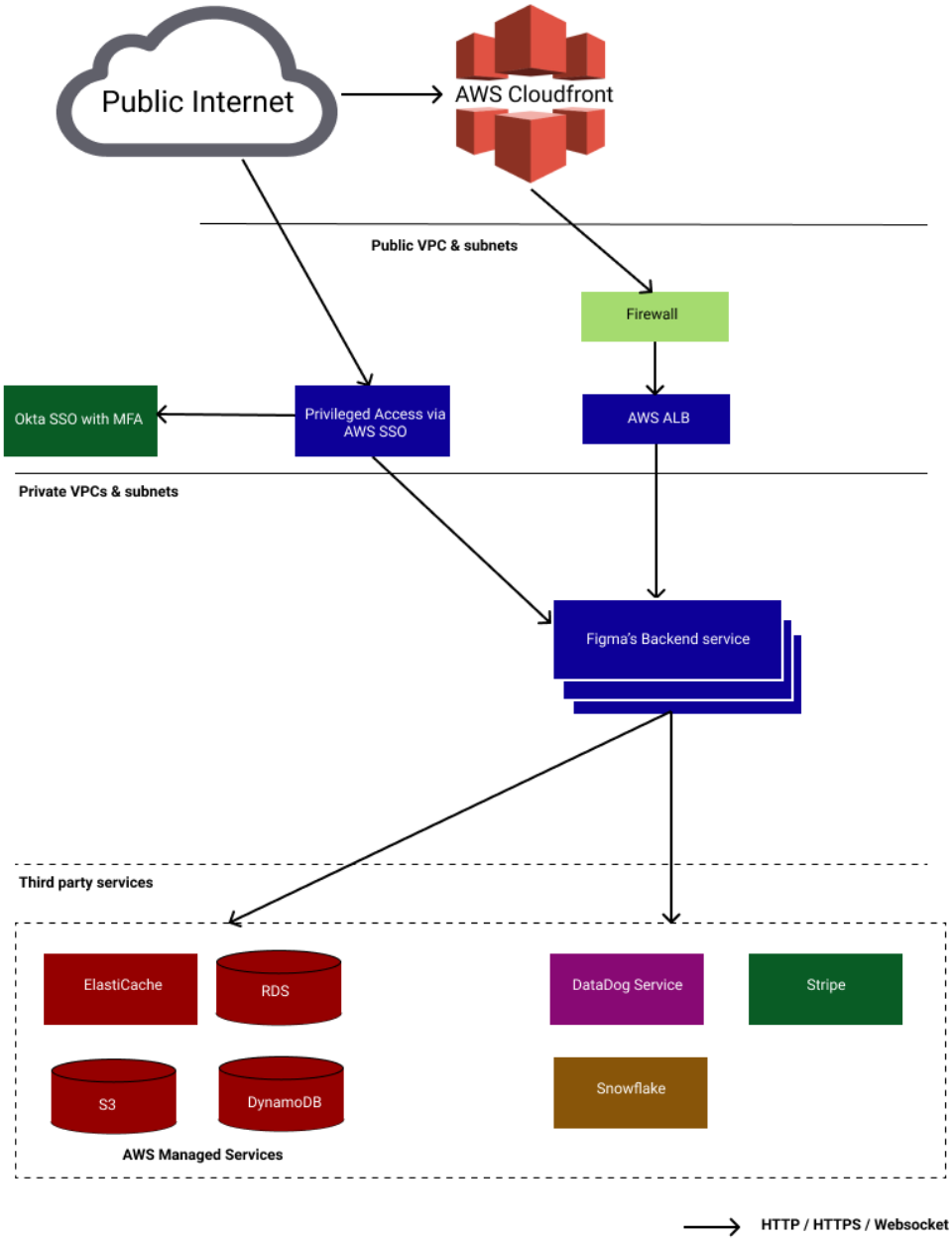

Figure 1: Figma's Infrastructure

Data storage: AWS S3, RDS, and DynamoDB are managed services provided by AWS. AWS RDS is the primary store for user data and meta-data of design files. AWS S3 is the primary datastore for images and contents of design files created with Figma. All customer data is encrypted at rest, backed up, and replicated.

Load balancers and network connections: Load balancers and network connections are managed within AWS. Figma's production environment is protected by virtual private cloud ("VPC"). Customer traffic into and out of the production environment uses Transport Layer Security ("TLS") connections to secure data in transit.

Application servers: The Figma application servers run on AWS EC2 and use encrypted Elastic Block Store ("EBS") volumes. AWS security groups are used to restrict communication between servers, and VPC is used to isolate the production environment from other environments.

Network

Figma's production network is maintained within AWS where Figma makes extensive use of security groups to enforce separate zones for different services. The corporate network is based on a wireless network and macOS endpoints. Fleetsmith is used to manage and administer security policies for workstations and laptops. Transmission of data is governed using multiple systems. Figma uses the TLS protocol for transmitting data over unsecured networks.

Database

Figma's primary database is AWS RDS, which is hosted and managed by AWS. Data is encrypted at rest and backed up continuously. Backup snapshots are stored for 14 days. This enables point in time recovery in the event of a major incident.

User data is also indexed within AWS ElasticSearch for faster searching, which is also hosted and managed by AWS.

User design files and attachments are stored in AWS S3, and each design file and attachment are logically segregated in the database.

Software

System configuration and provisioning software provide engineering teams with the capability to deploy secure and consistent configurations across different systems. This provides the ability to rapidly provision standard configurations and hardened baseline configurations for deployment of the Service.

Source code management software (such as GitHub) provides engineering teams with a repository to centrally store and manage code used in production. This software allows code and scripts to be standardized and version controlled through the software development lifecycle that includes monitoring, testing, and approval of changes to maintain quality standards for code development.

An administrative console allows restricted employees to perform administrative tasks on customer accounts, such as those related to accounting, subscription, and product features. The administrative console only provides access to meta-data about the accounts and does not provide access to confidential customer data (i.e. design files). Customers must explicitly invite employees to access their design files (i.e., to help troubleshoot a problem). In the unlikely event that the user is unable to access or share their files, a limited number of senior engineering team members have the ability to download files using the administrative console upon consent by customers. Actions are logged and documented in a support ticket.

In addition, Figma utilizes the following third-party tools and services to support various processes:

- AWS S3 - File storage
- AWS RDS - Application storage
- Asana - Ticketing tool
- Checkr - Background check system
- CircleCI - Continuous integration and testing tool
- Datadog - Monitoring
- Detectify - Website vulnerability scanner
- Fail2Ban – Bruteforce prevention (effective until September 2020)
- FileVault – Encryption
- Fleetsmith – Device management
- Freshservice – Access requests
- GitHub - Code repository
- HackerOne – Bug bounty program
- Ironclad – Vendor management
- Lattice – HR performance review
- Malwarebytes - Anti-malware
- NavEx - Ethics helpline
- Okta - Identity and access management
- Osquery - Endpoint logging and host-based intrusion detection
- PagerDuty - Alerting and escalation tool
- Panther - Monitoring and alerting tool
- Sapling - HRIS
- Segment - Analytics
- Slack - Internal communication tool
- Snowflake - Data warehouse
- Sunlight – Learning and development
- Zendesk - Ticketing system

AWS is a third-party vendor. Figma performs a review of the SOC 2 report or any equivalent reports such as ISO certification for this vendor on an annual basis. The evaluation of the SOC 2 report includes an assessment of the complementary user entity controls, subservice organizations, and mapping of the controls to key risks to help ensure that the relevant key controls are implemented and operating effectively to meet the security objectives at Figma.

Management also assesses for any deviations identified to determine if the deviations impact the security objectives at Figma. If there are exceptions, Figma performs a review of the impact of the exceptions, and if needed, follows up with the individual vendor. The other tools and services are also third-party vendors; however, customer data is not stored in these applications. These are supporting and monitoring tools and are only applicable to support certain controls and criteria.

Data

Data, as defined for the Figma System, includes all electronic data or information submitted by the customer to Figma. Access to data is restricted to authorized personnel and access is granted after receiving proper approval from management. Figma has developed a privacy policy to help personnel determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Figma without proper authorization.

Customer data is logically segregated from other customers and is stored in AWS RDS and AWS S3. Customer data is encrypted at rest and in transit between Customer and Figma. AES-256 encryption is used for data at rest. During transit between Customer and Figma, server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. Any attempt to access Figma using insecure HTTP protocol is automatically redirected to use secure HTTPS protocol.

Additionally, Figma has separate environments for testing and production that are completely isolated at the network level. Figma creates test data that does not contain any customer related confidential information.

Organizational Structure

Figma has a well-defined organizational structure in place that defines organizational structures, lines of reporting, and areas of authority. Senior leadership reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.

The organizational structure consists of the following core functions that support the Figma System:

- Senior Leadership: responsible for product vision, overseeing company-wide activities, and attaining business objectives.
- Engineering: responsible for the development, testing, deployment, and maintenance of new code for Figma production applications.
- Human Resources (People Operations): responsible for the hiring, performance management, and administration of people-related processes for the Figma team.
- Customer Support: responsible for managing client interaction, expectations including client onboarding support, account management, and day-to-day customer support.

- Information Security: responsible for the design and implementation of security policies; management of information assets, threats, vulnerabilities, and incidents; and employee education regarding information security and privacy.
- Legal: responsible for setting contractual obligations with third-parties and technology partners/suppliers, including (i) negotiation and drafting of legal terms and conditions; (ii) ensuring compliance with internal contractual standards; and (iii) review of information security and privacy issues.
- Product Management: responsible for building features and products for customers as well as actively communicating changes to the external and internal stakeholders such as customers and employees, respectively.

To drive clarity and transparency in the hiring process, Figma has documented detailed job descriptions highlighting the roles, responsibilities, and skill requirements posted on their website for current open positions. The recruiting process includes formal in-depth employment interviews to determine if candidates have relevant qualifications to fulfill the required roles and responsibilities.

Figma has established formal agreements with contractors and customers. These agreements include confidentiality commitments applicable to Figma. Vendor contracts restrict disclosure of Figma's confidential data.

Policies and Procedures

Figma has developed policies and procedures to operate, maintain, and secure the System, and to achieve the American Institute of Certified Public Accountants ("AICPA") Trust Services Criteria for Security. The policies and procedures are reviewed annually and updated if necessary.

Written policies and procedures are in place that relate to (i) identifying and designating information as confidential; (ii) protecting confidential information from erasure or destruction; and (iii) retaining confidential information for only as long as is required to achieve the purpose for which data were collected and are being processed. Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.

Figma's management team is responsible for establishing Organizational and Information Security policies, standards, procedures, and guidelines supporting the functioning of controls and processes, which includes change control, acceptable use, access management, vendor management, vulnerability management, incident management and escalation process, and enforcement of procedures across the organization. Policies and procedures are reviewed annually by the appropriate stakeholders and are updated as needed to reflect changes in the operating environment. The most current versions of the policies and procedures are posted on the Figma intranet and are made available to employees for their review.

Complementary Subservice Organizations Controls

Figma contracts with Amazon Web Services ("AWS"), an IaaS service provider, which provides the following services supporting the System: physical safeguards, environmental safeguards, infrastructure support and management, and storage services supporting the System. The affected criteria are included below along with the expected minimum controls in place at the third parties.

Criteria	Controls
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning. IT access privileges are reviewed on a quarterly basis by appropriate personnel. User access to systems is revoked timely upon termination. Data is encrypted in transit in AWS.
CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Physical access to the computer rooms, which house the entity's IT resources, servers, and related hardware, is restricted to authorized individuals through a badge access system or equivalent, and monitored by video surveillance. Requests for physical access privileges require management approval. Documented procedures exist for the identification and escalation of potential physical security breaches. Visitors must be signed in by an authorized workforce member before gaining entry and must be escorted at all times.
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Changes are authorized, tested, and approved prior to implementation.

Management's monitoring control over sub-service providers

Due diligence procedures are in place upon engagement and at least annually for third-party service providers according to the Information Management Standard. The annual evaluation includes an assessment of the sub-service providers related SOC, ISO, Information Security Compliance Policies, response to Security & IT Questionnaire, or other attestation reports, as well as an impact analysis for any identified deficiencies.

Attachment B - Principal Service Commitments and System Requirements

Figma designs its processes and procedures related to the Figma System to meet its objectives for its web-based interface design tool, which allows users to create, design, and share interfaces between users. Those objectives are based on the service commitments that Figma makes to user entities, the laws and regulations that govern the provision of the Figma System and the financial, operational, and compliance requirements that Figma has established for the System.

Security commitments to user entities are documented and communicated in the terms and conditions within the sign-up page in Figma and through the Master Service Agreement ("MSA") with enterprise customers. The description of the service offering and the system delineating the boundaries and describing relevant components is documented on Figma's website and Figma's internal Wiki page. Customer responsibilities, including changes to security commitments to its customers, vendors, and internal users, are also communicated in the internal and customer-facing website.

Figma's security commitments include, but are not limited to, the following:

- Security criteria within the design of the Figma System that permits system users to access the information they need based on their role in the System while restricting them from accessing information not needed for their role
- Use of third-party vendors to help detect security and vulnerability issues, which allows Figma to address potential threats as soon as possible to minimize impact
- Use of malware and firewall protection to prevent access to or alteration of any information asset
- Use of encryption technologies to secure customer data at rest and in transit

Figma establishes operational requirements that supports the achievement of security commitments and other system requirements. Such requirements are communicated in Figma's policies and procedures, system operation and boundaries, and terms and conditions with its customers. Information security policies are defined, posted, and available, delineating how systems and data are protected. These include policies around how the System is operated, how employees are hired and trained, the use of encryption technologies to protect customer data at rest and in transit, and a formal process to grant and revoke access to customer data.